UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,018	02/05/2002	Cheryl L. Beaver	SD-6823	1911

20567 7590 07/07/2006

SANDIA CORPORATION
P O BOX 5800
MS-0161
ALBUQUERQUE, NM 87185-0161

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/072,018	BEAVER ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9-11,18-20 and 24* is/are allowed.

6)☒ Claim(s) *1-8,12-17,21-23 and 25-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 03 May 2006.

2. Claims 1-27 are pending for examination.

3. Claims 1-8, 12-17, 21-23, 25-27 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The 35 U.S.C. 112 rejection involving the phrase "random number" in claims 1-3,13,25,26 and associated dependent claims, is withdrawn.

The 35 U.S.C. 112 rejection involving the phrase "absolute" in claim 22 is withdrawn.

The 35 U.S.C. 112 rejection involving the phrase "relative" in claim 23 is withdrawn.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-8, 12-17, 21-23, 25-27 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al, U.S. Patent 6,327,652 B1.

5. As per claim 1; "A method of performing electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, the method comprising the steps of:

generating a plurality of random numbers [figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., pseudo-random data structures), as broadly interpreted by the examiner, clearly encompasses the 'plurality of random numbers' aspects of the claim.];

distributing in a digital medium the plurality of random numbers to

the members of the group [figures 1-11 and associated descriptions, whereas the signed components are distributed to the users/network node processing elements, insofar as the customers of the DRM content of which the secure operating system components form the environment from which the content is so accessed, as broadly interpreted by the examiner, clearly encompasses the '...distributing in a digital medium ... group ...' aspects of the claim.];

publishing a hash value of contents of the digital medium [figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., hashed components prior to the cryptographic signing process) and subsequent hash/certificate verification prior to allowing the secure operating system components to process the DRM

functions, as broadly interpreted by the examiner, clearly encompasses the 'publishing a hash value ...' aspects of the claim.];

distributing to the members of the group

public-key-encrypted messages each containing

a same token comprising

a random number [figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., hashed components prior to the cryptographic signing process) and the public key certificate contains a certificate signing authority/entity private key signed verification content (common token element that is commonly distributed), as broadly interpreted by the examiner, clearly encompasses the '...distributing ... group ... public-key-encrypted messages ... token ... random number' aspects of the claim.]; and

encrypting a message with a key generated from

the token and

the plurality of random numbers [figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, as broadly interpreted by the examiner, clearly encompasses the 'encrypting a message ... token ... random numbers' aspects of the claim.].".

6. Claim 2 ***additionally recites*** the limitation that; "The method of claim 1 wherein the generating step comprises

generating at least approximately 20,000 random numbers.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., pseudo-random data structures), of which the client base for which distribution is to occur is clearly greater than 20,000 users (i.e., installed secured operating systems per se, each with art least a signed secure operating system component), as broadly interpreted by the examiner, clearly encompasses the 'plurality of random numbers ... approximately 20,000 ...' aspects of the claim.).

7. Claim 3 ***additionally recites*** the limitation that; "The method of claim 2 wherein the generating step comprises

generating 256-bit random numbers.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., pseudo-random data structures), of which the client base for which distribution is to occur is clearly greater than 20,000 users (i.e., installed secured operating systems per se, each with art least a signed secure operating system component, of which said component would generally be greater

than 256 bits (32 bytes)), as broadly interpreted by the examiner, clearly encompasses the 'plurality of random numbers ... approximately 20,000 ... 256-bit random ...' aspects of the claim.).

8. Claim 4 ***additionally recites*** the limitation that; "The method of claim 1 wherein the step of distributing in a digital medium comprises

distributing in a removable digital medium.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the components, of which the client base for which distribution is to occur is clearly a function of the digital medium distribution software which, as broadly interpreted by the examiner, clearly encompasses the 'distributing ... digital medium ... removable ... medium' aspects of the claim.).

9. Claim 5 ***additionally recites*** the limitation that; "The method of claim 4 wherein the step of distributing in a digital medium comprises

distributing in a medium selected from the group consisting of

CD-ROMS and

DVD-ROMS.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the components, of which the client base for which distribution is to occur is clearly a function of the digital medium distribution software which is embodied on CD-ROM and other associated removable optical memory technologies, as broadly interpreted by the

examiner, clearly encompasses the 'distributing ... digital medium ... removable ... medium ... CD-ROMS...' aspects of the claim.).

10. Claim 6 ***additionally recites*** the limitation that; "The method of claim 1 wherein the steps of publishing a hash value comprises

employing a Secure Hash Algorithm.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., hashed components prior to the cryptographic signing process) and subsequent hash/certificate verification prior to component transfer (i.e., utilizing associated data structure storage, via X.509, and SSL transfer; both using SHA hashing services/functionality), and subsequent allowing the secure operating system components to process the DRM functions, as broadly interpreted by the examiner, clearly encompasses the 'publishing a hash value ... Secure Hash Algorithm' aspects of the claim.).

11. Claim 7 ***additionally recites*** the limitation that; "The method of claim 1 additionally comprising the step of

rejecting a digital medium received by a user if

a hash value of contents of the received digital medium does not equal

the published hash value of the contents of the distributed digital medium.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions if so verified, else, rejected (i.e., not used as an operating system component for the DRM services), as broadly interpreted by the examiner, clearly encompasses the 'rejecting ... medium ... does not equal ... published hash value ...' aspects of the claim.).

12. Claim 8 ***additionally recites*** the limitation that; "The method of claim 1 wherein the step of distributing a token

is performed daily.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions such that ephemeral keys used for the certificate verification functions, as broadly interpreted by the examiner, clearly encompasses the 'distributing a token ... performed daily ...' aspects of the claim.).

13. Claim 12 ***additionally recites*** the limitation that; "The method of claim 1 wherein the encrypting step comprises

employing symmetric key encryption.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions such that private/session keys

(i.e., symmetric encryption), as broadly interpreted by the examiner, clearly encompasses the '... symmetric key encryption' aspects of the claim.).

14. Claim 13 ***additionally recites*** the limitation that; "The method of claim 1 wherein the encrypting step comprises

choosing randomly one of the plurality of random numbers.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., pseudo-random data structures), so that the DRM functions become a function of the 'pseudo-random data structures', as broadly interpreted by the examiner, clearly encompasses the 'choosing randomly ... plurality of random numbers' aspects of the claim.).

15. Claim 14 ***additionally recites*** the limitation that; "The method of claim 13 additionally comprising the step of

sending the encrypted message with

an index to the randomly chosen number and

a timestamp sufficient to enable a recipient to determine

a proper decryption token.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., hashed

components prior to the cryptographic signing process) and subsequent hash/certificate verification prior to component transfer (i.e., utilizing associated data structure storage, via X.509, and SSL transfer; both using inherent referencing of signed components for actual secure operating system components utilization), and subsequent allowing the secure operating system components to process the DRM functions such that ephemeral keys used for the certificate verification functions (i.e., inherently timestamp), as broadly interpreted by the examiner, clearly encompasses the 'encrypted message ... index ... number ... timestamp ... proper decryption token' aspects of the claim.).

16. Claim 15 ***additionally recites*** the limitation that; "The method of claim 1 wherein the group is a domain.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed components are distributed to the users/network node processing elements, insofar as the customers of the DRM content of which the secure operating system components form the environment from which the content is so accessed, and further, the group receiving the DRM content via a network infrastructure (i.e., the Internet; an inherently domain oriented network architecture), as broadly interpreted by the examiner, clearly encompasses the '...group is a domain' aspects of the claim.).

17. Claim 16 ***additionally recites*** the limitation that; "The method of claim 1 wherein one or more members of the group is a domain.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed components are distributed to the users/network node processing elements, insofar as the customers of the DRM content of which the secure operating system components form the environment from which the content is so accessed, and further, the group receiving the DRM content via a network infrastructure (i.e., the Internet; an inherently domain oriented network architecture, of which sub-elements of the Internet, are themselves domains), as broadly interpreted by the examiner, clearly encompasses the '...group is a domain' aspects of the claim.).

18. Claim 17 ***additionally recites*** the limitation that; "The method of claim 1 wherein anonymity of a sender of the message is maintained.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, and further encompassing use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), as broadly interpreted by the examiner, clearly encompasses the 'anonymity ... sender ... message is maintained' aspects of the claim.).

19. Claim 21 ***additionally recites*** the limitation that; "The method of claim 1 wherein the method provides

absolute anonymity for communications between the members.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, and further encompassing use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), as broadly interpreted by the examiner, clearly encompasses the 'absolute anonymity ... between the members' aspects of the claim.).

20. Claim 22 ***additionally recites*** the limitation that; "The method of claim 21 wherein the method provides

anonymity

as to authorship of the communications and

as to electronic mail routing of the communications.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, and further encompassing use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), as broadly interpreted by the examiner, clearly encompasses the 'anonymity ... between the members' aspects of the claim.).

21. Claim 23 ***additionally recites*** the limitation that; "The method of claim 1 wherein the method provides

anonymity for communications between the members

by not providing for communications between

members of the group within a same domain.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, and further encompassing use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), as broadly interpreted by the examiner, clearly encompasses the 'anonymity ... between the members' aspects of the claim.).

22. As per claim 25; "A method of performing anonymous electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, the method comprising the steps of:

generating a plurality of random numbers [figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., pseudo-random data structures), and further encompassing use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), as broadly interpreted by the examiner, clearly encompasses the 'plurality of random numbers' aspects of the claim.];

distributing in a digital medium the plurality of random numbers to

the members of the group [figures 1-11 and associated descriptions, whereas the signed components are distributed to the users/network node processing elements, insofar

as the customers of the DRM content of which the secure operating system components form the environment from which the content is so accessed, as broadly interpreted by the examiner, clearly encompasses the '...distributing in a digital medium ... group ...' aspects of the claim.]; and

encrypting a message with a key generated from

a token and

the plurality of random numbers while

maintaining anonymity of authorship of the message [figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, and further encompassing use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), as broadly interpreted by the examiner, clearly encompasses the 'encrypting a message ... token ... random numbers' aspects of the claim.].".

23. As per claim 26; "A method of performing anonymous electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, but wherein said communications are revocable, the method comprising the steps of:

generating a plurality of random numbers [figures 1-11 and associated descriptions, whereas the signed secure operating system components insofar as signing via a public key encryption process thereby generating uniquely signed components (i.e., pseudo-random data

structures), further encompassing the use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), and further use of the said public key encryption process whereas the revocation of certificates via ACL services, as broadly interpreted by the examiner, clearly encompasses the 'plurality of random numbers' aspects of the claim.];

distributing in a digital medium the plurality of random numbers to

the members of the group [figures 1-11 and associated descriptions, whereas the signed components are distributed to the users/network node processing elements, insofar as the customers of the DRM content of which the secure operating system components form the environment from which the content is so accessed, as broadly interpreted by the examiner, clearly encompasses the '...distributing in a digital medium ... group ...' aspects of the claim.];

encrypting a message with a key generated from

a token and

the plurality of random numbers [figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, and further encompassing use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication), as broadly interpreted by the examiner, clearly encompasses the 'encrypting a message ... token ... random numbers' aspects of the claim.]; and

permitting revocation of the message by a revocation authority comprising

one or more of the members [figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, further encompassing the use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication) and further use of the said public key encryption process whereas the revocation of certificates via ACL services, as broadly interpreted by the examiner, clearly encompasses the 'encrypting a message ... token ... random numbers' aspects of the claim.].".

24. Claim 27 ***additionally recites*** the limitation that; "The method of claim 26 wherein the permitting step

maintains anonymity of authorship of the message.".

The teachings of England et al suggest such limitations (i.e., figures 1-11 and associated descriptions, whereas the signed secure operating system components signed, distributed, encrypted/decrypted, and verified for use in the DRM functions, further encompassing the use of the CPU ID public key signing aspects of the signed/verified components (i.e., assured anonymous CPU ID with authentication) and further use of the said public key encryption process whereas the revocation of certificates via ACL services, as broadly interpreted by the examiner, clearly encompasses the 'permitting revocation ... maintains anonymity of authorship' aspects of the claim.).

Allowable Subject Matter

25. Claims 9-11, 18-20, 24 are allowable over prior art.

Conclusion

26. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100